

Les objets connectés représentent-ils un risque ? | Denis JACOPINI



Les #objets connectés représentent-ils un risque ?

Contrôler sa maison ne son aspectement du bout des doigts, utilisé, soit la promesse des fameux objets connectés. Des réfrigérateurs ou télévisions, en passant par les thermostats, les caméras de surveillance, les serrures, ou encore les éclairages, de plus en plus d'équipements de foyer peuvent être pilotés à distance à l'aide d'un smartphone via un réseau local et Internet. Mais derrière ce rêve de la maison intelligente et connectée, combien d'insécurités il y a quelques années, au contact d'objets promettant de sécurité. Et des Lises.

Le marché se déchaîne

Depuis l'invention des technologies futures, le bâtiment comme valement à se déstructurer grâce à l'émergence des appareils et objets connectés. Après les équipements multimédias (Smart TV, systèmes Wi-Fi, imprimantes...), les appareils électroménagers connectés - réfrigérateurs, lave-linge, cafetières, robots, etc... commencent à débarrasser sur le marché. Mais ce sont surtout les systèmes prêts à l'emploi ou les modules démontables permettant de connecter l'éclairage, les serrures de portes, les stores, les systèmes de surveillance (caméras, détecteurs de mouvement/fumée, alarmes)... ou encore le chauffage qui concentrent un succès grandissant.

«L'arrivée au marché de la maison intelligente est l'aboutissement d'un vœu de nos nombreux clients, mais également par leur prix de plus en plus abordable. Toutefois, comme s'agissait quel appareil quel se connecte à un réseau Wi-Fi et Internet, ils s'exposent de fait à toutes sortes de risques. D'autant que pour la plupart, ils ne possèdent aucun système de protection de type antivirus, antimalware, etc. Des failles de sécurité, plus ou moins importantes en fonction de la nature des objets, qui ont été soit démontrées par des experts de sécurité, soit expliquées par des hackers. Nous verrons les cas les plus étonnants qui donnent matière à réflexion.

Des appareils sous haute surveillance

Derrière les incidents récents liés à la sécurité des objets connectés est devenue un sujet particulièrement sensible depuis la médiatisation d'un meter de recherche public nommé Ignited Shadow. Créé par un Américain du nom de John McWherty, ce dernier explore le Web en continu pour référencer et regrouper tous les appareils qui y sont connectés. Quelques clics suffisent pour trouver aussi bien des systèmes domestiques, que des smartphones, des ordinateurs, des télévisions, voire des installations industrielles sensibles telles que des centrales électriques, des raffineries, ou encore des usines.

Pas de quoi rassurer les utilisateurs, même si à l'origine Shadow n'aurait pas été créé pour nuire, mais au contraire pour aider les experts et sécurité à identifier les vulnérabilités des logiciels et infrastructures réseaux des entreprises. Le service se charge de garder une trace de tous les faits et gestes de ses utilisateurs, qui doivent obligatoirement s'identifier et souscrire à un abonnement au-delà d'un certain nombre de recherches. Il n'est resté pas moins que désormais, tout objet connecté ayant une adresse IP peut être localisé, identifié, voire détourné.

Les promesses de la maison intelligente et connectée

Contrôler et gérer divers équipements de la maison à l'aide d'un smartphone, d'une tablette ou d'un ordinateur n'est plus une utopie. Intéressé d'essayer à tirer des câbles partout et d'entreprendre de lourds et coûteux travaux avec des spécialistes. Tout le monde peut en principe concevoir une installation domestique soit-même grâce à la nouvelle génération de produits disponibles sur le marché. Au-delà du confort qu'offrent ces nouvelles technologies et pratiques, elles permettent de réaliser de substantielles économies d'énergie, de renforcer la sécurité du foyer, ou encore de se prémunir d'accidents domestiques (incendie, inondation...).

Confort, sécurité, prévention, économie d'énergie.

Domotique

Les produits ont évolué, mais la promesse de la domotique est toujours la même : centraliser et automatiser grâce à diverses technologies l'ensemble ou une partie des équipements électriques du foyer. Des services qui se font à distance, des caméras et des détecteurs de mouvement capables de s'adapter en votre absence et de vous envoyer des SMS en cas d'intrusion, des thermostats intelligents permettant de gérer la température au degré près dans chaque pièce, des stores électriques qui s'ouvrent et se ferment automatiquement en fonction de la lumière, des détecteurs de fumes obligatoires dans toute l'habitat européenne à partir de mars 2015 qui lancent des alertes en cas de départ d'incendie, des éclairages qui courent différentes ambiances lumineuses selon les heures de la journée, les possibilités sont quasi-illimitées.

Réaliser une installation domestique est maintenant à la portée du plus grand bricoleur grâce, notamment, à ce qu'on appelle les kits domotiques. Ces systèmes prêts à l'emploi qui s'installent dans tous les espaces de bridage et d'électronique (Automatisme, Lenz, Merlin, Electro Dépt...) et même dans certains hypermarchés permettent de connecter et de contrôler à distance des équipements de la maison via une seule et même interface. Ces packs se composent d'un serveur domotique / multimédia (voir le réseau Wi-Fi du foyer), et d'un éventuel plus ou moins important d'équipements de surveillance, d'automatisation, de localisation, etc.

Ces dispositifs communiquent entre eux par le biais de différentes technologies sans fil comme le courant porteur (CPL), le Wi-Fi, les radiofréquences, ou des protocoles propriétaires. Pour les contrôler à l'aide d'une tablette ou d'un smartphone depuis le réseau local du foyer ou à distance par Internet, l'utilisateur n'a plus qu'à jouer du bout des doigts avec les icônes représentant les équipements connectés pour déclencher des actions déterminées ou déclencher.

Créer des scénarios

Dans le jargon de la domotique, un scénario désigne un ensemble d'actions programmées pour différents moments de la journée, de la semaine, de mois, voire de l'année. Les fabricants ont réalisé d'innombrables progrès pour faciliter la gestion des produits domotiques et la création de scénarios en développant des applications très intuitives. Exit les lignes de code informatique, ou les menus interminables ou vocabulaire incompréhensible, grâce aux icônes visuelles qui permettent de reconnaître les différents parties du foyer, et à des commandes simples de clic ou de glissement.

Point d'orgue des maisons intelligentes, les applications mobiles facilitent la compréhension et l'utilisation des équipements domotiques.

De quoi élargir, par exemple, au weekend, un scénario qui consistait à déclencher la mise à l'arrêt de l'eau, à partir de l'heure : ouvrir les stores, allumer la lumière d'un couloir, faire chauffer la cafetière, lancer la radio, débrancher les portes, débrancher les caméras de surveillance, etc. Bien entendu, toutes les solutions domotiques s'offrent pas les mêmes possibilités. Les fabricants distillent généralement des packs spécialisés dans une seule partie (surveillance, automatisation, éclairage, chauffage...) à compléter au fur et à mesure. En parallèle, il existe d'innombrables objets connectés autonomes (stations météo, balances Wi-Fi, robots intelligents, ampoules connectées...) qui se connectent directement au réseau du foyer, sans passer par un serveur propriétaire.

Aura, le réveil intelligent de Withings qui analyse votre sommeil pour vous réveiller en douceur

La production, ce n'est que tout ce qui est possible. Les développeurs de l'application, qui résident au contact d'Apple et Google pour que tous les appareils connectés puissent communiquer entre eux via leurs plateformes mobiles respectives, ne sont pas encore d'actualité. À moins de choisir du matériel très haut de gamme comme le box universelle Lifesense Vision (2 999 euros) compatible avec la plupart des protocoles de communication des solutions domotiques (ZigBee, Bluetooth, Wi-Fi, etc.), vous avez à équiper chez le même fabricant pour pallier les éventuels problèmes de compatibilité.

Aura, le réveil intelligent de Withings qui analyse votre sommeil pour vous réveiller en douceur.

Depuis quelques mois, la sécurité d'Internet des objets fait beaucoup d'écouter. Au quatre coins de la planète, des experts en sécurité prennent le sujet à bras le corps : ils multiplient les démonstrations pour montrer la vulnérabilité de certains produits et la façon dont les cybercriminels pourraient les exploiter pour réaliser des attaques. Les spécialistes n'ont pas tort d'alerter les fabricants, car les risques ne sont pas seulement virtuels. Depuis quelques mois, quelques cas concrets d'attaques basées sur des objets connectés présentent le bien-fondé de leurs craintes.

Failles et vulnérabilités des objets connectés

La division de sécurité Fortify du Bureau de constructeur HP a récemment publié un rapport alarmant sur la sécurité des objets connectés. Elle a ainsi annoncé avoir découvert plus de 25 vulnérabilités sur 30 objets connectés parmi les plus populaires (Smart TV, thermostats intelligents, balances, mais domotiques...). Sans donner plus de précision sur les marques concernées, elle déclare que la plupart ne crypte pas les données téléchargées sur le réseau et n'ajoute pas de mot de passe sécurisé avant caractères spéciaux et chiffres pour l'accès à distance. Ces dispositifs autorisent des tiers de passe comme « 123456 » particulièrement vulnérables (un fait que nous avons effectivement pu vérifier après quelques recherches sur Shodan). Par ailleurs, la protection de leurs logiciels serait insuffisante, car non chiffrée, et certaines applications Web ne sont pas de fait sécurisées.

Toujours selon ce rapport, 98 % des produits analysés collectent des informations personnelles sensibles (adresse email/postale, date de naissance), acceptables de circuler en clair sur Internet à cause du manque de protection. Difficile néanmoins de contester un rapport ne présentant pas les modèles et les marques des appareils concernés. À travers cette étude, la division déclare vouloir sensibiliser les auteurs du marché, mais elle souhaite aussi promouvoir sa solution de sécurité Fortify on Demand auprès des fabricants.

C'est pas la seule étude de ce type, la plupart de chercheurs indépendants d'AN-Tech avait mis en lumière d'importantes failles de sécurité, notamment sur les systèmes domotiques (Smart TV de Mediatek, et XXXX MAX 1 d'Hama, permettant de contrôler le chauffage, l'électricité, les prises de courant avec interrupteur, ou encore l'éclairage. Ainsi incroyable que cela puisse paraître, leur communication n'était pas sécurisée sur le réseau local de leur domicile. Comme, mais en plus, la solution d'Internet ne sécurisait aucune authentification que cela soit pour l'accès local ou via Internet.

Avec un moteur de recherche comme Shodan, l'exploit qui aurait pu repérer les vulnérabilités de la marque sur Internet et en prendre la distance, étonnant. Gageons que les deux fabricants ont pris les mesures qui s'imposent pour sécuriser un tant soit peu leurs systèmes.

Le Logis Kertec sécurisé ? Pas tout à fait.

En France, le réseau Kertec, les experts réalisent des « exploits », c'est-à-dire des tests (appelés Proof-of-concept, preuve de concept) visant à démontrer la présence de vulnérabilités sur des systèmes ou des logiciels pour préparer des attaques. Certains exemples sont particulièrement convaincants. La spécialiste Jennifer Savage avait ainsi montré comment elle avait réussi à exploiter une faille de sécurité du fameux logiciel multifonctions Kertec qu'elle avait offert à sa fille. Cela lui avait permis de prendre le contrôle à distance de l'appareil à son insu, à l'aide d'un ordinateur, et d'utiliser sa caméra et son miroir pour l'espionner.

Puis récemment, des chercheurs ont découvert une faille de sécurité dans les contrôle d'ampoules connectées Lifi en exploitant une faille de leur protocole de communication. Ils ont pu démontrer qu'ils pouvaient théoriquement s'introduire dans le rayon de 30 mètres dans le réseau Wi-Fi domotique appelé Lifi sans être connectés et accéder à des données privées stockées sur d'autres appareils du foyer, par exemple. Depuis cette découverte, le fabricant s'est efforcé de publier un correctif.

Des Smart TV qui espionnent les télégraphes

Les démonstrations les plus impressionnantes ont eu lieu lors des conférences Black Hat organisée chaque année à Las Vegas, mais aussi à Amsterdam ou à Tokyo. Elles réunissent aussi bien des chercheurs, des experts en sécurité, que des hackers de haut vol. En 2013, plusieurs conférences ont exposé les vulnérabilités des TV connectées. L'un d'entre eux a prouvé notamment qu'il était possible de prendre le contrôle de la caméra et du micro d'une Smart TV et d'espionner leur propriétaire à leur insu. Et cela, même quand l'appareil était éteint.

Le thermostat Nest Lab qui joue les « Big Brother »

À l'occasion de la dernière édition de cet « été d'été » au mois d'août 2013 à Las Vegas, des chercheurs d'une université de Floride ont montré comment pirater le thermostat intelligent de Nest (la start-up rachetée par Google). Avec un accès physique à l'appareil (évidemment), ils ont pu prouver qu'il est possible d'insérer un code pour détourner et récupérer les informations recueillies par l'appareil, sans que son propriétaire s'en aperçoive.

Nouvelle génération de cyberattaques

La sécurité et la protection des données privées ne sont clairement pas la priorité de certains acteurs du marché des objets connectés. Sans vouloir dresser un tableau catastrophique de la situation, les cyberattaques sur les objets connectés présentent des failles de sécurité ont tendance à se multiplier ces derniers mois. Caméras de vidéosurveillance, réfrigérateurs, balades, Smart TV, voici quelques exemples connus d'appareils qui ont fait l'objet d'attaques diverses et variées.

Des caméras au service des espions

Responsable de ne pas citer la faille de sécurité qui avait permis à des hackers de diffuser sur Internet le flux vidéo de milliers de webcams et caméras de vidéosurveillance Trendnet, installées chez des particuliers. Malgré la publication rapide d'un correctif par le fabricant après sa découverte, de nombreux utilisateurs continuaient en un plus tard à être exposés à leur insu, car ils n'avaient toujours pas fait la mise à jour.

De hauts dirigeants dans le bureau d'un meurtrier

Début 2014, la société spécialisée en sécurité ProofPoint a révélé pour la première fois une cyberattaque réalisée à partir de toutes sortes de dispositifs connectés dont des Smart TV, des MAC, des consoles de jeux vidéo, un réfrigérateur, etc. Les pirates auraient exploité leur vulnérabilité pour installer un serveur de spam (botnet) et envoyer plus de 750 000 emails frauduleux. Sans l'état de l'Ohio aux États-Unis ou le Mex d'avril dernier, un hacker s'a-t-on trouve au milieu que de pirater un baladeur pour terroriser un bébé et ses parents. Et prouver le contrôle de l'appareil équipé d'un caméra, d'un micro et d'un haut-parleur, il s'est mis à harceler des centaines sur le courrier.

La collecte et collecte de données en règle

En France, le Réseau Numérique, le Réseau numérique en développement informatique comme sous le nom de l'Organisation a fait une découverte. Suite à l'acquisition d'une Smart TV de la marque LG, il a remarqué l'apparition de publicités ciblées comme un point en voir sur des services Web tels que Gmail. Il en a donc déduit que la TV devait forcément analyser ses habitudes, les programmes qu'il regarde, les sites qu'il visite, etc. Cherchant à savoir plus, il constate en fait que ce téléviseur dispose d'une fonctionnalité de collecte d'informations de vidéos.

Même après avoir désactivé cette fonction, le téléviseur continuait de transmettre des informations à son insu à LG. Le constructeur ne se contentait pas de surdoser ses habitudes de consommation, mais il récupérait également des données personnelles telles que des vidéos de famille qu'il avait projetées sur son écran depuis son ordinateur. En scandale donc se serait bien passé si qui aurait, depuis, décidé de permettre à ces clients de « restaurer » descripteur l'option de collecte de données. Derrière le manque de sécurité constaté sur de nombreux objets connectés, il faudra donc aussi développer un secteur des pratiques strictes de certains fabricants.

Source: l'Organisation de l'Organisation

Sous l'œil de Shodan

En reliant un tour d'horizon des objets connectés pour la maison, susceptibles de présenter des risques, on ne peut conclure qu'ils sont tous potentiellement vulnérables. Certains ne sont pas sécurisés ou pas suffisamment, tandis que d'autres présentent des failles de sécurité plus ou moins importantes peuvent être exploitées pour mener des attaques externes ou à courte distance. Mais la principale faille qu'exploitent les hackers est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup d'ont pu constater des risques et s'efforcer d'activer la sécurité de leurs équipements, ou se contentent de laisser les dispositifs par défaut fournis par les fabricants. Or, une pratique, d'autant qu'un peu de recherche comme Shodan, tous les appareils connectés ont une adresse IP visible sur Internet.

D'une efficacité réduite, le service permet d'effectuer des recherches globales, ou par pays, en réalisant une simple requête pour identifier, localiser, ou encore rendre le contrôle des appareils connectés non protégés par un mot de passe. Il suffit de saisir le nom d'une marque de produits connectés comme (Dlink, Netgear, Samsung...) ou de cliquer sur les mots recherchés les plus populaires (Webcam, Camera, Netcam...) pour voir apparaître leurs adresses IP et y accéder. Le service dispose d'un moteur de recherche sur les dispositifs, mais n'est pas sécurisé, protégé ni non par des identifiants, etc.

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique

Un accès facile et direct à une adresse IP publique